Hastings Communications and Entertainment Law Journal

Volume 25 | Number 1 Article 2

1-1-2002

Facing the Music: The Dubious Constitutionality of Facial RecognitionTechnology

John J. Brogan

Facing the Music: The Dubious Constitutionality of Facial Recognition Technology

by
JOHN J. BROGAN*

* Information Technology Analyst, University of Iowa Office of Information Technology. I would like to thank Evan Seamone and Nick Johnson for their helpful insights on earlier drafts of this manuscript.

I. Introduction

National identification cards are again in the news;[1] in the wake of the events of September 11, the political climate seems ripe for the adoption of stricter identification measures.[2] Proponents of such a system point to its value as a tool for the protection of innocent individuals[3] and downplay its significance as a vehicle for monitoring individual activities.[4] Opponents fear the growing shadow of the government's surveillance schemes encroaching on the privacy of individual citizens,[5] particularly in light of the fact that such a system

1. Kathryn Balint, *Attack on America: Personal Technology*, San Diego Union Tribune (Mar. 11, 2002) at E1, available at 2002 WL 4590778.

2. *See* Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 41 (Winter 2002) (arguing that even before September 11th, the intersection of a number of federally legislated databases was already pushing us toward a National Identification System and contending that the post-September 11th pressures will virtually ensure a widespread identification system). Polls taken shortly after the attacks suggested that "70 percent of U.S. citizens favor[ed] the creation of a national identification system." *U.S.-Attacks Oracle Offers Free Software for National I.D. System*, EFE NEWS SERVICE (Sep. 24, 2001) at ____, *available* at _____. More recent polls suggest that support for such an invasive system is waning. The Electronic Privacy Information Center (EPIC) reports that

> [t]wo recently published polls show that support for a national ID card has decreased. Results from a poll on the February 27 Washington Post Federal Page showed that public opinion was divided on the issue, with 47% of Americans believing a national ID "would make electronic transactions with the government and business faster and more secure" and "would be an easier way for people to verify their identity in places such as airports and government offices," while 44% thought of it as "a way to keep track of people" and "an invasion of people's civil liberties and privacy." A new survey released on March 12 by Gartner Inc. found that 26 percent of Americans are in favor of a national ID card, while 41 percent oppose the idea.

EPIC, *National I.D. Cards*, at <http://www.epic.org/privacy/id_cards/> (last visited Apr. 12, 2002). *See also* Julia Scheeres, *Support for I.D. Cards Waning*, WIRED, available at <http://www.wired.com/news/print/0,1294,51000,00.html> (last visited Apr. 12, 2002) (noting that public acceptance of such a system hinges on the likely uses of the system).

3. *See generally* Thomas G. Donlan, *"Secure in Their Persons": A National Identity Card is No Threat to Liberty*, BARRON's (Mar. 18, 2002) at 43, available at 2002 WL-BARRONS 7653943.

4. *See id.* "But the fear is misplaced in the 21st century. Americans may fear tyranny, and oppose every hint or possibility that it may emerge. But an identity card is not tyranny, it is an identity card. Free citizens may very well wish to prove their identity, and a government composed of free citizens may even require them to do so at times."

5. The American Civil Liberties Union (ACLU) has continuously opposed national identification cards, fearing that

> [a] national I.D. card would essentially serve as an internal passport. It would create an easy new tool for government surveillance and could be used to target critics of the government, as has happened periodically throughout our nation's history. While the Social Security Act originally contained strict prohibitions against use of the Social Security card for unrelated purposes, over the past 50

would be unlikely to provide material limitations on terrorist activities within the United States.[6]

As it stands, the government already has all of the resources that are necessary to monitor individual citizens in all aspects of their daily lives: omnipresent video cameras;[7] extensive databases replete with medical, financial, and criminal information;[8] and facial matching technology.[9] Combined, this technology provides unprecedented power to identify, record, and monitor the most intimate details of human life: the places we go, the activities in which we engage, and the people with whom we associate.[10] Admittedly, this technology is

> years those prohibitions have been ignored or legislated into oblivion and restrictions on a national I.D. card would follow the same path.

ACLU, *Why Does the ACLU Oppose a National I.D. System?*, at <http://www.aclu.org/library/aaidcard.html> (last visited Apr. 12, 2002). Notably, the context in which national identification continually arose prior to September 11th was in relation to the need to control illegal immigration. *Id.* The attacks of September 11 intensified the national perception that identification cards are necessary to curb the movements of terrorists. EPIC, *National I.D. Cards*, *supra* n. 2.

6. *See id.* (noting that "ID cards won't thwart future terrorist attacks . . . because the criminals will still be able to purchase fraudulent documents, such as birth certificates, that would be needed to obtain the IDs. Privacy advocates also fear that the cards themselves would act as a kind of national passport, allowing authorities to monitor people's movements and activities. EPIC and other groups believe that increased information-sharing among government agencies is just as insidious as having to fork over your ID card to cops who think you look 'suspicious.'").

7. *See* N.Y.C. Surveillance Camera Project, *Project Summary*, at <http://www.mediaeater.com/cameras/summary.html> (last visited Apr. 12, 2002) (noting that "[o]ver the last five months, a small but dedicated group of New York Civil Liberties Union volunteers walked the streets of Manhattan in search of video surveillance cameras. This group sought out every camera, public or private, which records people in public space. From the records they made of the camera locations, the volunteers produced a comprehensive map of all 2,397 surveillance cameras in Manhattan.").

8 *See* Sobel, *supra* n. 2, at 41-45 (noting the omnipresence of databases available today).

9. *See infra* nn. 83-89 and accompanying text.

10. For instance, consider the remarks made on a recent episode of the *McLaughlin Group*:

> MR. MCLAUGHLIN: To Americans, that chilling request is the image long associated with national identity cards. But the image may be changing, as a result of September 11th. A Harris Poll conducted immediately thereafter found that 68 percent of Americans favored a national I.D. system. Even renowned civil rights influentials support a national I.D. Quote, "We need to distinguish between a right to privacy, which I believe in, and a right to anonymity, which I no longer believe in," unquote . . . . Under review are so-called smart cards, especially biometric cards like scans of the retina and fingerprints. The scans are linked to databases. The Department of Defense is already issuing smart cards to more than 4 million service members.
>
> Senator Dick Durbin of Illinois, a Democrat, has introduced a bill to create a national standard for drivers' licenses, which could become a de facto national

not perfect;[11] our privacy may currently be protected, to some extent, by the technological and infrastructural limitations of these systems.[12] This protection is of little comfort, however, given the rapid improvements being made to the technology,[13] and to the extent that these systems are prone to error, a malfunctioning system may only increase the likelihood that citizens will be subjected to false identifications and harassment.[14]

The growth of biometric identification,[15] and in particular facial scanning technology,[16] raises serious questions about the continued longevity of a variety of Constitutional protections.

In this article, I argue that the deleterious effects of facial scanning technology may be curtailed by distinguishing between wide area facial scans[17] and focused facial scans.[18] Recognizing this distinction, courts should determine that wide area scans are *per se* unconstitutional, while focused scans serve a legitimate law

I.D. card. Representative Jim Moran, also a Democrat, will introduce a bill that carries it a step further, requiring biometric data.

The McLaughlin Group (Broadcast, Mar. 30-31, 2002)

11. According to one privacy advocate,

> [t]hose new converts to the cause of "security" may have switched sides too soon. Modern surveillance cameras aren't just monitored by bored policemen - they're often connected to computer software that's supposed to "recognize" faces stored in databases of criminal suspects. An ACLU study of Tampa's experience with the technology found that "the system made many false matches between people photographed by police video cameras . . . and photographs in the department's database of criminals, sex offenders, and runaways." That shouldn't be a surprise. In a 2000 U.S. Defense Department test of face-recognition products, reportedly the best false-detection rate found was 33 percent.

J.D. Tucille, *The Fight Over Photos*, available at <http://www.free-market.net/spotlight/cameras/> (last visited Apr. 12, 2002).

12. *Id.*

13 Barnaby J. Feder, *Face-Recognition Technology Improves*, N.Y. Times (March 14, 2003) C2.

14 A recent example of how the limitations of biometric identification could be problematic for individuals was demonstrated in the relative ease that an individual could be subjected to identity theft.

15. Biometric identification systems measure and analyze the physical characteristics of the human body, including recognition of: fingerprints, handprints, voice patterns, retinal patterns, brainwaves, physiognomy, etc.

16 The reason why facial scanning is so much more invidious than most other types of biometric identification is the fact that an individual need not be aware that they are being subjected to identification. Unlike a retinal, hand, or fingerprint scan, where an individual must knowingly accede to identification, facial recognition is passive in that it requires no knowledge on the part of the person being scanned.

17. *See infra* Part III.B.2.a.

18. *See id.*

enforcement purpose when supported by a minimal level of suspicion that a particular individual is engaged in criminal activity.

Part II of this article considers the background of biometric identification, tracing the lineage of technological evolution from the early approaches of criminologists to modern crime databases. The section then moves to a consideration of the component parts of facial scanning: surveillance, recognition, and information synthesis. Part III considers the validity of facial scanning as a Fourth Amendment event under the Constitution, examining critical cases decided by the United States Supreme Court from *United States v. Katz* through *Kyllo v. United States*. Part IV argues that the generic category of facial scanning should be bifurcated into two different types of scans: wide area scans and focused scans. It then proposes that wide area scans should be severely limited or banned and that focused scans should only be available to law enforcement when police are seeking to identify or pinpoint the location of an individual suspect for whom they have a minimal amount of suspicion or knowledge of past or future criminal activity.

II. Background

A. The Historical Origins of Biometric Identification

Biometric identification is not a new phenomenon in law enforcement. Almost as long as scientists have been aware that each human being has certain physical attributes that are unique to that individual, criminologists have taken advantage of that fact to aid them in the investigation of crimes. The first recorded incident of biometric identification was Alphonse Bertillon's database of criminals in Nineteenth Century Paris.[19] Bertillon recorded various physical statistics: the length of a criminal's finger and the circumference of his head in an effort to quickly identify recidivists.[20]

Bertillon's system quickly evolved and the recognition of fingerprints as a means of identification opened new doors for investigating criminal activity.[21] But the true breakthrough in biometric databases has been the advent of the digital age.

A collection of information is only as useful as the ability to organize it efficiently and access it rapidly. Moreover, the growing

19. Simon Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* 40 (2000).

20. *Id.*

21. Simon Cole, *A History of Fingerprinting and Criminal Identification* 11 (2001).

transience of society makes it necessary to have multiple sinks of information that are both self-contained and integrated. The databases must be self-contained in order to quickly access a limited amount of information based on its geographical relevance; it must be integrated in order to allow law enforcement agencies to access a broader field of information on individuals moving through different jurisdictions.

The necessity of solving these two problems became clear to police departments in the mid-1980s that were struggling under the weight of excess information. In Los Angeles in 1985, a manual match of an anonymous fingerprint would require an examination of over 1.7 million fingerprint cards, a Sisyphean task for a single worker.[22]

The answer to this problem is the utilization of a series of decentralized but connected databases, known as a distributed database.[23] The distributed database achieves the two needs of law enforcement by being both self-contained and interoperable. As a result, local police can quickly identify a fingerprint by first checking the print in their local computer system before broadening the scope of the search to other jurisdictions.[24]

While fingerprinting is probably the most common and widely known form of biometric identification, it is by no means the only example. A variety of forms of biometric identification have now become commonplace, including retinal recognition,[25] handprint

22. *See* David Johnston, *Computer Could Point Finger at Murderers: Automated Searches Through Fingerprint Files Could Substantially Increase Arrests in L.A.*, L.A. TIMES (June 28, 1985) at ____ (pointing out that the task of identifying a single fingerprint using a computerized system could accomplish in five minutes what an individual technician would need 67 years to complete).

23. According to the Institute for Telecommunications Sciences, a distributed database is "not entirely stored at a single physical location, but rather is dispersed over a network of interconnected computers."). Institute for Telecommunications Sciences, *Definition of a Distributed Database*, <http://www.its.bldrdoc.gov/fs-1037/dir-012/_1750.htm> (last visited Apr. 2, 2002).

24. *See generally* Neil Munro and Elizabeth Frater, *The Digital Dragnet*, THE NAT'L JOURNAL, Mar. 23, 2002, at 2002 WL 7094871:

There are between eight and 20 federal criminal databases, including the Justice Department's National Crime Information Center (which stores criminal records and arrest warrants) and the Combined DNA Index System (which stores convicted felons' DNA "fingerprints"). The nation's 16,000-plus police jurisdictions also maintain an array of databases . . . . These store data on more than 59 million individual offenders-far more than the federal agencies store. . . . The nonfederal databases are increasingly linked to local government databases created by municipal courts, parole services, and public defenders' offices.

25. For instance, the state of Kansas has tentatively approved a change to the issuance of driver's licenses that would contain biometric identifiers. *See* Chris Ochsner,

scans,[26] and DNA matching.[27] In addition, other databases have proliferated throughout the public and private sectors that contain a vast quantity of somewhat overlapping information.[28] As a result, a surprisingly complete portrait of an individual can be gleaned from the trivial linkage of just a few databases.

A full examination of just how much information these databases track is beyond the scope of this article; however, one commentator has suggested that

> the database problem cannot adequately be understood by way of the Big Brother metaphor—even when adapted to account for private sector databases. Although the Big Brother metaphor certainly describes particular facets of the problem, . . . [the more apropos metaphor is] Franz Kafka's depiction of bureaucracy in THE TRIAL—a more thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information.[29]

B. The Components of Facial Scanning

Turning from the question of databases generally to the more specific consideration of using these databases for law enforcement purposes, it is important to begin by examining the underlying steps involved in a particular scan.

A database of information, in itself, tells us very little about future activity. Although it is sometimes useful in predicting future events from patterns of empirical criminal behavior, the real goal of maintaining a large amount of biometric information is to reconstruct the past.

Investigators arrive at a crime scene and must attempt to piece

Bill Would Require Fingerprint to Apply for Driver's License, TOPEKA CAPITAL JOURNAL (Mar. 12, 2002) at C3, available at 2002 WL 4880417 ("Under the proposal, the Division of Motor Vehicles would keep a database of ''biometric identifiers,'' which could include a thumbprint, retinal scan, face recognition or hand geometry.").

26. *Id.*

27. Robert W. Schumacher II, *Expanding New York's DNA Database: The Future of Law Enforcement*, 26 FORDHAM URB. L.J. 1635, 1644 (1999).

28. *See* McGregor McCance, *Device Keeps Problems in Check; Fingerprinting Frustrates Forgers*, RICHMOND TIMES-DISPATCH (Mar. 3, 2002) at E-8, available at 2002 WL 7193592 (describing how convenience store owners are beginning to use fingerprint scans and biometric databases to catch check forgers).

29. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (2001).

together what happened at that location from small clues: a fingerprint, a strand of hair, skin cells, or semen. In each case, a piece of physical evidence taken from a crime scene is checked against existing records to determine if a match exists. If a match is found, the investigator's job is made easier; if not, the information is stored in the computer and available for future cataloguing and cross-checking.

At an abstract level, the database scan involves three steps. First, baseline information is entered into the database. This information could be fingerprint information, DNA information, or something else entirely. The information may be obtained through some standard arrest procedure,[30] from a professional regulatory body,[31] from an insurer, or by alternative means. Second, comparison information must be acquired from another source. Lifting fingerprints or other DNA information from a crime scene is one way in which comparative data might be acquired. Third, the two pieces of information must be checked against each other. This is the phase at which an individual or a computer checks the anonymous comparative data against the baseline data and determines if the two pieces of biometric data originated from the same source. The outcome of such an analysis is binary; that is, at the end of the process one is left with a statement that is either true or false. The two pieces of biometric information came from the same person or they did not.

Facial scanning operates much like other forms of biometric

30. One commentator has described the process of police fingerprinting in some detail, stating that

> [w]hen the local police arrest a suspect, they normally fingerprint the suspect. They take at least one set of fingerprints each on an FD-249 and an R-84 and also record other relevant data on both cards. If the local police do not immediately resolve the offense (for example, the suspect must await trial), they send the fingerprint card (FD-249) to the CJIS, but keep the R-84 for future use. When the CJIS receives the FD-249, it enters the information in the NCIC. When the charges against the suspect are resolved (for example, by conviction), the police fill in the disposition on the retained R-84 and send it to the CJIS. The CJIS then matches the R-84 to the previously sent FD-249 and updates the information on the NCIC, including the conviction. If the CJIS, for whatever reason, cannot locate an FD-249 for the suspect for that particular offense, the CJIS returns the R-84 to the submitting agency. Once entered in the NCIC, the information about the suspect, including the conviction, is available to all other authorized agencies for their use.

Major Michael J. Hargis, *Three Strikes and You Are Out – The Realities of Military and State Criminal Record Reporting*, 1995-SEP ARMY LAW. 3, 5 (1995).

31. For instance, in order to join the bar in some states, one must submit to fingerprinting. *See* Alaska Bar Association, *Reciprocity Application and Instructions*, available at <http://www.alaskabar.org/526.cfm> (last visited Apr. 2, 2002).

identification. In order to make the system work, there must first be a database of baseline images against which the comparative image can be examined.[32] The comparative image must then be acquired from an input source and analyzed against the baseline data. On the surface, these processes look very similar, but as one looks more closely, the differences become clear.

III. Facial Scanning as a Fourth Amendment Event

A. Katz and Its Progeny

1. United States v. Katz[33]

The Fourth Amendment to the United States Constitution guarantees that individuals shall be free from "unreasonable searches and seizures."[34] A substantial amount of judicial time and effort has been expended developing the legal contours of what constitutes a search. The seminal case on this issue is *United States v. Katz*, which laid the foundation—in Justice Harlan's concurrence—a seemingly simple two-pronged test.[35] The test provides that a governmental action constitutes a search if an individual has a subjective expectation of privacy and if society is willing to objectively recognize that expectation as reasonable.[36]

Katz broke from prior law in that it shifted from an interpretation of the Fourth Amendment that focused on sacrosanct spaces to a broader view of privacy as tied to the individual.[37] But as much as *Katz* gave in the way of an expanded notion of privacy, it sustained an important caveat: that society is not prepared to concede the existence of privacy where the action in question is openly displayed to the public.[38] As a result, that which is done or said in a space that can be viewed or overheard by a member of the general

32. *See Smart Cards Could Cut Airport Wait Times for Frequent Flyers*, AIRLINE INDUSTRY INFORMATION (U.K.) (Apr. 1, 2002) ("The cards would store personal information about the holder on a magnetic strip or computer chip and they would be used in conjunction with biometric measurements such as a scan of the user's iris, face, hand or fingerprint. At security checkpoints, the person would submit to at least one biometric measurement, the results of which would be compared to an image stored in a database or on the card itself.").

33. 389 U.S. 347 (1967).

34. U.S. CONST. amend. IV.

35. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

36. *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

37. *Katz,* 389 U.S. at 351.

38. *Id.* at 361 (Harlan, J., concurring).

public is not off limits to law enforcement officials merely because they are an arm of the government.

Two of the Court's subsequent cases demonstrate how large an exception the public view doctrine carves into the Fourth Amendment.

2. Smith v. Maryland[39]

In *Smith v. Maryland*, the Court held that an individual did not have a reasonable expectation of privacy in the phone numbers he dialed.[40] *Smith* involved a case in which the phone company—at the request of police but without a warrant from a magistrate—placed a pen register on Smith's telephone line in order to ascertain what numbers he was dialing.[41] Smith sought to suppress evidence obtained from the pen register, arguing that he had a subjective expectation of privacy in the phone numbers he dialed and that his expectation was reasonable.[42]

The Court disagreed, arguing that society is unwilling to accept that there is a reasonable expectation of privacy in the phone numbers one dials.[43] Pointing to the fact that people are generally aware that the phone company keeps track of long distance numbers for billing purposes, the Court found that the use of a pen register to track local numbers produced no additional incremental invasion of privacy.[44] In addition, the Court asserted that because a phone number does not expose the content of the actual phone conversation and is not content in itself, it does not constitute a search within the meaning of the Fourth Amendment.[45]

The potential impact of *Smith* in light of the growing necessity of the Internet, and more specifically e-mail, as a form of communication is unclear. A number of scholars have already expressed concern about justifying the constitutionality of the Carnivore[46] system on *Smith*.[47] Although a lengthier discussion of

39. 442 U.S. 735 (1979).
40. *Id.* at 742.
41. *Id.* at 739, n.4
42. *Id.* at 742.
43. *Id.*
44. *Id.*
45. *Id.*
46. The FBI e-mail surveillance system, Carnivore, works like a kind of Internet wiretap that tracks emails and other electronic communications. Agents use it only after obtaining a court order that allows them to intercept the communications of a criminal suspect. The FBI then install the specialized computer on the networks of Internet providers, where it "sniffs" out all mail and records sent to or from the target of an

these issues is beyond the scope of this article, it is nevertheless important to recognize that as the law currently stands, the utilization of technology to intercept information traveling through the public domain does not amount to a constitutional search event under the Fourth Amendment.[48]

This sobering realization provides two alternatives. The first possibility is that non-content based communications will never be protected by the Fourth Amendment. Alternatively, an information transfer may constitute a search, but requires something more than the trace of a numerical signature,[49] as in *Smith*, to invoke constitutional protection.[50] It is to this latter possibility that we will return later in this section.[51]

3. California v. Ciraolo[52]

In *Ciraolo*, the Court considered the issue of whether an overflight of a person's backyard that is surrounded by a high fence constitutes a search under the Fourth Amendment.[53] In making the threshold determination, the Court considered the two factors established in *Katz*: Did Ciraolo have a subjective expectation of privacy regarding the curtilage of his home and, if so, was society

investigation. Chris Oakes, *ACLU: Law Needs 'Carnivore' Fix*, WIRED (July 12, 2000), available at <http://www.wired.com/news/politics/0,1283,37470,00.html> (last visited April 2, 2002).

47. *See generally* Christian David Hammel Schultz, *Unrestricted Federal Agent: 'Carnivore'and the Need to Revise the Pen Register Statute*, 76 NOTRE DAME L. REV. 1215, 1219 (2001) (discussing the need to revise the pen register statute so as to de-link Carnivore from *Smith*).

48. Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDIS. L.J. 295, 299 (1999).

49. I use the phrase "numerical signature" rather than phone number to sidestep the issues presented by Carnivore as discussed in note 46.

50. As the Court articulated in *Smith v. Maryland*,

> a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications. This Court recently noted: "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed . . . a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."

Smith, 442 U.S. at 741 (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977)).

51. *See infra* Part III.A.4.

52. 476 U.S. 207 (1986).

53. *Id.* at 209.

prepared to accept that expectation as reasonable?[54]

The Court gently waffled its way past the first issue, pointing out that although the high fences and the geographic proximity of the marijuana crop to his home evidenced some subjective expectation of privacy, Ciraolo had not engaged in the most privacy-protecting conduct.[55] For instance, the Court remarked that Ciraolo did not attempt to hide his gardening activities from the view of someone standing on top of a double-decker bus or truck.[56] As such, the Court concluded that a mere hope that no one will see into an enclosed space is different than a subjective manifestation of privacy.[57]

The Court disposed of the objective prong more easily, concluding that because the public routinely flies over property in commercial airplanes, society is unprepared to recognize the belief that one's property is free from aerial surveillance as objectively reasonable.[58]

Ciraolo is particularly interesting for our purposes on two levels. First, it is a case that deals with a space that has long been considered deserving of the greatest level of protection from government intrusion – the home and the areas immediately adjacent to it. Second, it is not a case that squarely addresses the technology issue, even though it is essential to the disposition of the case.[59]

The space question can be dismissed quickly, albeit not perfunctorily. What *Ciraolo* apparently tells us is that even the most sacred spaces are not immune from the government's prying eyes. To wit, if you want to sunbathe nude in your backyard, build a roof over it. But if our expectations of privacy regarding our own backyards are unreasonable, what can we expect of spaces away from the home? The answer, seemingly, is very little.

Second, *Ciraolo* aptly demonstrates one of the primary sources of concern about the Court's current interpretation of searches under the Fourth Amendment—that the ever-expanding power of technology will continue to erode objective notions of privacy to the

54. *Id.* at 212.

55. *Id.*

56. *Id.* at 211.

57. *Id.* at 212.

58. *Id.* at 213. Justice Powell's vigorous dissent poses an alternate view. "In my view, the Court's holding rests on only one obvious fact, namely, that the airspace generally is open to all persons for travel in airplanes. The Court does not explain why this single fact deprives citizens of their privacy interest in outdoor activities in an enclosed curtilage." *Id.* at 216 (Powell, J. dissenting).

59. *Id*. at 213-14.

point that even the most significant invasions of privacy will be commonplace.[60] In *Ciraolo*, the notion that air transportation had become, at the time of the decision, so ubiquitous as to negate an objective expectation of privacy is telling.[61] It suggests that the Court may be less concerned with technological encroachments whose primary purpose is not surveillance-oriented. Thus, the airplane is not as threatening a technological intrusion as the spike mike, even if the functional result of both is to diminish privacy.

The result of this reasoning is both confusing and ironic. The Court has consistently ruled that enhancing technologies do not constitute searches under the Fourth Amendment.[62] Binoculars merely enhance what an officer could see with his own eyes;[63] night vision goggles do much the same. Dog sniffs expand upon the sense of smell.[64] But barring an argument that airplanes just expand on our ability to flap our arms, it's hard to see what justifies the intrusion. The pressures that erode privacy can therefore be seen as bi-directional: general technology raising the objectivity bar while sense-

60. *See generally* Kyllo v. United States, 533 U.S. 27, 33-34 (2001) (discussing the circularity of relying on an objective expectation of privacy that constantly shifts under the pressure of new innovations).

61. Justice Berger's opinion in *Ciraolo* expresses this notion explicitly when he remarks that:

> [o]ne can reasonably doubt that in 1967 Justice Harlan considered an aircraft within the category of future "electronic" developments that could stealthily intrude upon an individual's privacy. In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet. The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.

476 U.S. at 215. Justice Scalia's majority opinion in *Kyllo v. United States* reiterates this point all too clearly:

> [i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

533 U.S. 27, 33-34 (2001) (citations omitted).

62. *See generally* Alyson L. Rosenberg, *Passive Millimeter Wave Imaging: A New Weapon In the Fight Against Crime or a Fourth Amendment Violation?*, 9 ALB. L.J. SCI. & TECH. 135 (1998).

63. *See* David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 20-22 (1996).

64. *See generally United States v. Place*, 462 U.S. 696 (1983).

enhancing technologies narrow the breadth of protection.

4. Kyllo v. United States[65]

The Court's most recent grapple with the threshold search question was in *Kyllo*. At issue in that case was whether a thermal scan of Kyllo's residence constituted a presumptively unreasonable search requiring a warrant under the Fourth Amendment.[66]

Writing for the majority, Justice Scalia concluded that the scan was an unreasonable search. In making this determination, the Court retraced its previous decisions, emphasizing the test cobbled from *Katz* that there must be a subjective expectation of privacy that is determined to be objectively reasonable.[67] Bracketing *Smith* and *Ciraolo* as cases where the defendant failed to meet his objective burden under the *Katz* test, the majority took particular exception to two aspects of the scan involved in *Kyllo*.

First, the Court emphasized its longstanding commitment to the home as a particular zone of privacy worthy of the greatest degree of protection.[68] Within that space, it found that individual and societal expectations of privacy are at their zenith.

Second, given the importance of the protected space, the Court held that the use of specialized technology to acquire information about the interior activities of a home, normally obtainable only from a warranted search, was unreasonable per se. In making this determination, the majority refused to accept the Ninth Circuit's analysis, adhered to by the dissent, that there is a discernible distinction between devices that monitor data emanating from a home as opposed to technologies that scan its interior. Justice Scalia rejected the government's position that

> there is a fundamental difference between what it calls "off-the-wall" observations and "through-the-wall surveillance." But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house-and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that

65. 533 U.S. 27 (2001).
66. *Id.* at 29.
67. *Id.* at 33.
68. *Id.* at 31.

> reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home.[69]

In the wake of *Kyllo*, a critical question remains: Does the Court's decision apply only to specialized technologies aimed at the home? In the narrowest reading, it seems that it would. The majority is particularly concerned with intrusions into the home.[70] But a slightly broader reading could offer supporters of privacy more hope.

The Court's notion of objective privacy hinges on whether or not the technology performing the scan is in general use by the public.[71] Furthermore, the reaffirmation of *Katz* in the *Kyllo* decision suggests that notions of privacy remain tied to the individual rather than the space.[72] As a result, although it's clear from the decision in *Kyllo* that the reason why the Court is quick to invalidate the search is because it intrudes into the home, it does not follow that the home is the only locus of protection; it just means that applying the rationale of *Katz* to other spaces is more problematic.[73]

Operating within the framework established by *Kyllo* and its predecessors, the possible constitutional challenges to wide area facial scans begin to emerge more clearly.

B. To Scan or Not to Scan?

After the incidents of September 11, law enforcement officials

69. *Id.* at 35-36.

70. *Id*. at 31.

71. The majority remarks that

> obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is *not in general public use*. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.

Id. at 34-35 (emphasis added) (citations omitted).

72. *Id.* at 32-33.

73. Justice Scalia notes that

> [w]hile it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences are at issue, in the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*.

Id. at 34 (emphasis in original).

are under extreme pressure to protect against future catastrophes.[74] In this climate, numerous means of crime prevention have been bandied about, including national identity cards and state-sanctioned torture.[75] Focusing on facial scanning as one of these preventive strategies, this section considers whether or not such an activity rises to the level of a search under the Fourth Amendment.

Before directly answering the question, it is worthwhile to spend some time looking at where the technology stands today—where it is being deployed, how it is being used, and who is watching.

1. Scanners, Scanners Everywhere . . .

In early 2001, some 72,000 fans attending Superbowl XXXV were facially scanned while entering the turnstiles of Raymond James Stadium in Tampa.[76] Using technology called FaceTrac, 128 points of each attendee's face were scanned and checked against an FBI crime database.[77] Although no arrests were made, 19 known criminals were identified as a result of the scan.[78] At the time, privacy groups condemned the government's actions,[79] but in the wake of the World Trade Center attacks, resistance to the use of this technology is quickly fading away.[80]

In fact, a number of airports in various cities already have the technology in place, including: Tampa,[81] London,[82] Fresno,[83]

74. Molly Ivins, *Post Sept. 11: For Those Who've Lost Their Common Sense*, CHIC. TRIB., Nov. 15, 2001, at 31, available at 2001 WL 4135953; Rene Sanchez, *Border Patrol Agents Answer Higher Call*, WASH. POST, Dec. 2, 2001, at A12, available at 2001 WL 30329602.

75. Conor O'Clery, *A Strange Turn-up for the Book*, IRISH TIMES (Feb. 16, 2002) at 59, available at 2002 WL 12662419 (citing Harvard law professor Alan Dershowitz as one such proponent of these schemes).

76. Mark Hollands, *We Don't Need IT to Make Us Stupid*, THE AUSTRALIAN, Feb. 13, 2001, at 48.

77. *Id.*

78. *Id.*

79. Robert Trigaux, *In Riskier World, Personal Security Trumps Personal Privacy*, ST. PETERSBURG TIMES, Feb. 24, 2002, at 1H, available at 2002 WL 12607101.

80. An October 2001 Harris Poll indicated that "86 percent of respondents favored the use of facial recognition devices to scan for terrorists in public places." Kathryn Balint, *No 'Snooper-Bowl' for San Diego Police: Won't be Using Face-Scanning Technology That Sparked Ire in Tampa*, SAN DIEGO UNION-TRIBUNE, Jan. 20, 2003, at E1, available at 2003 WL 6561326.

81. *Biometrics: A Security Boon or Invasion of Individual Privacy*, CORRECTIONS PROFESSIONAL, Mar. 25, 2002.

82. *Id.*

83. *Biometrics' Time Has Come*, COLLECTIONS AND CREDIT RISK, Feb. 2002, at 8.

Providence,[84] Kansas City,[85] Boston,[86] and shortly Washington D.C.[87] Virginia Beach is using the technology at the Ocenfront to track "runaways, wanted felons and people suffering from dementia."[88] In San Francisco, at least 30 high-resolution cameras are being installed at every Bay Area Rapid Transit (BART) stop to scan passengers moving throughout the city.[89]

Remarking on the growing omnipresence of cameras, former National Security Agency counsel Stewart Baker suggested that "'George Orwell underestimated our enthusiasm for surveillance. . . . He correctly predicted we'd have cameras everywhere. What he failed to imagine is that we'd want them so bad[ly] we'd pay for them.'"[90]

This mentality is reflected by security specialists preparing for potential terrorist strikes on sports arenas, who are eager to use face scanning devices like the ones operated at the Superbowl in Tampa.[91] Furthermore, "[f]acilities managers are working closely with law enforcement, watching for" danger signs like "[m]eetings and public protests by dissident groups."[92]

In short, public support for increased security measures is so high that the political checks that should operate to preserve privacy measures cannot reliably operate. As such, it is the judiciary who will likely have to take a leading role in safeguarding the general public from itself.

2. Making Facial Scanning a Search

By all indications, convincing courts to treat facial scanning as a search under the Fourth Amendment is at least an uphill battle, and at most, impossible. At least one commentator addressing the issue

84. Mary Kirby, *More U.S. Airports Acquire Visionics Biometric Systems*, AIR TRANSPORT INTELLIGENCE, Jan. 24, 2002.

85. *Id.*

86. *Id*.

87. *See supra* n. 80.

88. Warren Fiske, *House Panel Backs Face-Scanning Limit*, THE VIRGINIAN-PILOT, Feb. 8, 2002, at B4, available at 2002 WL 5486691.

89. David Streitfeld & Charles Piller, *A Changed America; Big Brother Finds Ally in Once-Wary High Tech*, Los Angeles Times (Jan. 19, 2002) at A1, available at 2002 WL 2447524.

90. *Id.*

91. Edward Iwata, *Stadium Security Gets Serious*, U.S.A. TODAY, Mar. 18, 2002, at 3B, available at 2002 WL 4722024.

92. *Id*.

suggests that facial scans are unlikely to rise to the level of a search.[93] As discussed earlier, the public view doctrine established in *Katz* and subsequently expounded in *Smith* and *Ciraolo* probably encompasses all of the spaces in which an individual might be subject to a facial scan.[94] Because airports, public transit stations, and sport stadiums are all open spaces in which an individual's face could be readily viewed and identified by a police officer, the use of a video camera to achieve the same end, arguably, is no different.

In spite of this fact, I argue that wide area facial scans should rise to the level of a search for two reasons. First, as a practical matter, the scans enable access to so much more information than would be available to the public view of the police officer that some level of Fourth Amendment protection seems necessary. Second, to the extent that an analogy is possible, facial scans operate much like a consensual encounter between civilians and law enforcement officials. But unlike a stop-and-identify situation where a person is free to refuse a policeman's request, the lack of consensuality involved in facial scanning—notably, the inability to refuse the encounter—produces a constitutionally significant event.

a. Approaching the Problem

As mentioned, finding a precise analog between wide area facial scans conducted by computers and traditional forms of police activity is difficult because the scans have an amorphous quality that is difficult to characterize precisely. In particular, the level of invasiveness of a scan depends, in large part, on the way the system works.

For instance, the FaceIt system developed by Visionics, Inc. is capable of recognizing single or multiple faces in either one-to-one or one-to-many matching mode.[95] Depending on the implementation of the system, authorities may have access to a relatively small pool of images in the database[96] or an extremely large number.[97]

93. Milligan, *supra* n. 48, at 318.

94. *See supra* Part III.A.1.

95. Identix, *Faceit Face Recognition Technology*, available at <http://www.indentix.com/newsroom/whatisfaceit.html> (last visited Mar. 3, 2003).

96. *See* William Welsh, *Facing Trouble*, WASHINGTON TECHNOLOGY, at <http://www.washingtontechnology.com/news/16_21/state/17781-1.html> (last visited Mar. 3, 2003) (reporting that the Tampa system currently has only 900 entries in its database, but will soon expand to 45,000).

97. Visionics, Inc., *ID Solutions*, available at <http://www.visionics.com/faceit/apps/idsol.html> (last visited Mar. 31, 2002). ("There are estimated to be 1.1 billion facial images in identification databases around the world. No re-enrollment is required.")

Furthermore, depending on the level of integration, the system could return only the name of the individual or it could return cross-referenced data available in any linked database. This could potentially include any criminal information, tax information, credit information, health information, and vehicle registration information. Likewise, the database could be read-only, which would prevent the system from adding information, or it could be writable, allowing the system to automatically add certain details every time it found a match. This information could include the time at which the match was made, the location of the camera making the match, and possibly the images of individuals photographed shortly before or after a match. In effect, simply by hooking the right databases together, law enforcement officials could track the movements of an individual, the people with whom she associated, and any other information tied into the system. To give an extreme, but not unfathomable example, each time one stopped at a toll, stepped on the subway, passed through a turnstile, withdrew money from an ATM, or went to work, the system could keep a record, and this would be made possible by the mandatory photo identification issued by each state's Department of Motor Vehicles.

b. Applying the *Katz* analysis

Given the diversity of systems that can and have been implemented in various jurisdictions, coupled with the ease with which a system could be upgraded or downgraded as necessary, attempting to argue that particular versions of the system may or may not be legitimate would be futile. As such, this argument proceeds under the notion that a brightline rule is more appropriate than a case-by-case analysis for the purposes of categorizing any given facial scanning activity as an event under the Fourth Amendment.

Operating from this premise, we briefly revisit the dual-tiered requirement of *Katz*: that the government engages in a search when it violates an individual's subjective expectation of privacy that society is prepared to recognize as reasonable.[98]

1. The Subjective Prong

To what extent do individuals have a subjective expectation of not being facially scanned when they appear in public? The answer to this question necessarily depends on the individual. Nevertheless,

98. *Katz*, 389 U.S. at 361.

there are some fairly good reasons why any particular person might have a subjective expectation of privacy that he is not being scanned.

Conceding that most people have no subjective expectation that they will not be watched or captured on videotape as they move about in public, there must be something more that the individual is relying on in order to meet the first prong of *Katz*. One possibility is that although an individual expects to be seen by the government, he does not expect to be recognized by the government. That is, absent specific illicit conduct that would give the government a reason to learn his name, there is an expectation by all but the most paranoid elements of society that the government is not watching for "you in particular". Another possibility is that even if one expects to be identified, there is still no expectation that that identification will be tied to a veritable cornucopia of data detailing the most intimate details of one's life. In either case, most people would likely have some subjective expectation of privacy as they move about in public, even though that expectation is substantially less than they would expect in a more intimate space like the home.

2. The Objective Prong

The more difficult question is whether such an expectation would be recognized by society as reasonable. As discussed above, the Court's analysis of this prong is linked to two factors.[99] First, to what extent is the technology in question being used by the general public? Second, does the technology allow law enforcement to achieve an objective that would normally be circumscribed by the Fourth Amendment?

The first issue can be disposed with fairly easily. Although the individual elements of facial scanning technology are widely available: cameras, recognition software, and databases,[100] the power of a scanning system is its breadth: the dizzying quantity of interlinked cameras and baseline databases. To that extent, facial scanning systems are in no more common use by the general public than was the thermal sensing technology used in *Kyllo*.

The more difficult question is whether the technology provides

99. *See supra* Part III.A.4.

100. Mark Boal, *Spycam City*, THE VILLAGE VOICE (Oct. 6, 1998) at 38, available at 1998 WL 20492919. ("A hundred bucks at a computer store already buys face-recognition software that was classified six years ago, which means that stored images can be called up according to biometric fingerprints.").

an end run around the Fourth Amendment. Arguably, it does for a number of reasons. First, although law enforcement officials claim that facial scanning systems merely allow "machines to do what . . . [police have] always done" by "giv[ing] policemen pictures and put[ting] them on every corner,"[101] in truth the two activities are quite different.

Under the traditional method, police start with specific, articulable information: a person for whom they are looking; a reason why they are looking for that person. The police then take a photograph of that person and compare the face of each person that passes them against the baseline photograph. In the parlance of Visionics' technology, this is a one-to-one match: each new face is matched against one existing face.[102]

When the computer performs a wide area scan (or one-to-many match),[103] it engages in a task that no police officer individually, or any police force as a whole, could achieve. It examines each face against as many as a billion faces for a match.[104] But more importantly, it does so for no reason. A wide area scan is not looking for someone in particular; it is looking for anyone, suspicious or not, who happens to wander past. Furthermore, to the extent that the database tracks the location of faces it successfully scans, it operates as a homing device on a person's movements. In the words of one commentator:

> The new surveillance goes beyond merely invading privacy . . . to making irrelevant many of the constraints that protected privacy." For example, mass monitoring allows police to eliminate cumbersome court hearings and warrants. Immediately after a crime, cops check cameras in the vicinity that may have captured the perpetrator on tape. So, as surveillance expands, it has the effect of enlarging the reach of the police. Once it becomes possible to bank all these images, and to call them up by physical topology, it will be feasible to set up an electronic sentry system giving police access to every citizen's comings and goings.[105]

101. Warren Fiske, *House Panel Backs Face-Scanning Limit*, THE VIRGINIAN-PILOT, Feb. 8, 2002, at B4, available at 1998 WL 20492919.

102. *See supra* notes 95-97 and accompanying text.

103. *Id.*

104. Visionics, Inc., *ID Solutions*, *supra* n. 97.

105. Boal, *supra* n. 100 at 38.

Of course, the technology feared by that author in 1998 is now a reality.

c. The Nature of the Search

Accepting for the moment, *arguendo*, that a search has occurred, the question remains: what kind of search? The obvious problem is that a facial scan doesn't look like the kind of searches we're worried about - the kind where the contents of someone's house are rummaged while looking for a particular item.

In order to find the answer to this question, we have to look past the basic scan, the recognition of one picture against another, to what the scan really does: it correlates a data set, pinpointing where a particular person is a particular time. And more importantly, the cumulative effect of each identification is a more substantial intrusion; it is a map of human behavior, a list of the idiosyncrasies that make each person unique.

But even if the accretion and tracking of data regarding an individual's movement does not seem like the kind of search typically protected by the Fourth Amendment, the outcome of the facial scan appears less legitimate viewed through the lens of *Terry v. Ohio* and its progeny. In this section, I argue that wide area facial scanning operates as a kind of Fourth Amendment event that is short of a *Terry* stop, but is necessarily implied by the balancing analysis developed in — and subsequent interpretation of —*Terry*. In order to demonstrate this point, I briefly track a series of cases that define the basic contours of the law in this area.

C. Facial Scanning as a Fourth Amendment Event

A stop is a seizure under the Fourth Amendment[106] that is justified by an amount of suspicion less than probable cause.[107] It is one tool in an arsenal of weapons available to law enforcement to respond to "rapidly unfolding and often dangerous situations on city streets."[108] In *Terry v. Ohio*, the Supreme Court allowed a stop and frisk based on the reasonable suspicion of a police officer that Mr.

106. *Terry v. Ohio*, 392 U.S. 1, 16 (1968). ("It must be recognized that whenever a police officer accosts an individual and restrains his freedom to walk away, he has 'seized' that person.")

107. *Id.* at 27. ("[T]here must be narrowly drawn authority to permit a reasonable search for weapons for the protection of the police officer, where he has reason to believe that he is dealing with an armed and dangerous individual, regardless of whether he has probable cause to arrest the individual for a crime.")

108. *Id.* at 10.

Terry was preparing to engage in unlawful activity.[109] The Court held that the governmental intrusion of a stop and frisk is justified when a police officer can "point to specific and articulable facts which, taken together with rational inferences from those facts" are deemed objectively reasonable at the time of the intrusion.[110]

In essence, the creation of the balancing test in *Terry*[111] created a sliding scale of interaction between the individual and the police. In ascending order, we have the consensual encounter, the investigative stop, the quasi-arrest, and the custodial arrest. Because of the fluidity of defining what constitutes a stop, it is worthwhile to briefly examine this question in more detail.

1. What makes a stop a stop?

The Court began to flesh out the question of what constitutes a stop in *United States v. Mendenhall*.[112] That case involved an encounter between Mendenhall and Drug Enforcement Administration (DEA) agents at the Detroit Metropolitan Airport. Believing Mendenhall's actions to be consistent with the "drug courier profile,"[113] the agents stopped her and requested to see her identificationand airline tickets.[114] After noting a name discrepancy between the two requested items, she was asked to accompany one of the agents to the DEA office for further questioning.[115] Although she did not verbally agree to further inquiries, she did follow the agent to the office.[116] In turn, heroin was discovered on her person and she moved to suppress the evidence prior to trial.[117]

Refusing to grant Mendenhall's request to suppress, the Court held that the initial encounter between the government and the defendant was consensual and did not rise to the level of a seizure.[118] In determining the moment at which an individual is seized for the purposes of the Fourth Amendment, the court indicated that "a person is 'seized' only when, by means of physical force or a show of

109. *Id.* at 28.
110. *Id.* at 21-22.
111. *Id.* at 21.
112. 446 U.S. 544, 551-52 (1980).
113. *Id.* at 548 n.1.
114. *Id.* at 547-48.
115. *Id.* at 548.
116. *Id.*
117. *Id.* at 549.
118. *Id.* at 555.

authority, his freedom of movement is restrainted."[119] Elaborating further upon the standard, the Court reasoned that "[a]s long as the person to whom questions are put remains free to disregard the questions and walk away, there has been no intrusion upon that person's liberty or privacy as would under the Constitution require some particularized and objective justification."[120]

The physical requirement of being able to "walk away" in *Mendenhall* was amended in *Florida v. Bostick*, where the defendant was naturally restrained as a result of the fact that the questioning involved in that instance took place on a bus.[121] Nevertheless, the Court sustained the basic framework of *Mendenhall* and concluded that:

> Bostick's freedom of movement was restricted by a factor independent of police conduct — i.e. by his being a passenger on a bus. Accordingly, the 'free to leave' analysis on which Bostick relies is inapplicable. In such a situation, the appropriate inquiry is whether a reasonable person would feel free to decline the officers' requests or otherwise terminate the encounter.[122]

The net effect of the *Mendenhall-Bostick* inquiry is that a court must assess whether an individual had the ability to choose not to be subjected to questioning by the government. Put simply, the consensual encounter between the government and the individual hinges on the consent of the individual.

2. The Hodari *Problem*

The same term that the Court decided *Bostick*, it also ruled on *California v. Hodari D.*[123] *Hodari* involved a juvenile offender who fled from a police officer preparing to engage in a consensual encounter. The officer chased Hodari and just as he was about to intercept him, Hodari discarded a rock-like substance that police ultimately determined to be crack cocaine. In his motion to suppress the illicit drugs, Hodari argued that he had been constructively seized upon apprehension of the police officer's imminent physical control.

In another opinion authored by Justice Scalia, the Court rejected

119. *Id.* at 553.
120. *Id.* at 554.
121. *Florida v. Bostick*, 501 U.S. 429, 431 (1991).
122. *Id*. at 436.
123. 499 U.S. 621 (1991).

this argument, contending that seizure constitutes a literal "taking possession."[124] Under this analysis, a seizure is not effectuated until there is either "a laying on of hands or application of physical force to restrain movement, even when it is ultimately unsuccessful."[125]

The *Hodari* problem, in the context of facial scanning, is that when a computer scans an individual's face, no physical seizure occurs. Nevertheless, as mentioned above, the scan can be as or more intrusive than a physical stop. The lingering question, to which I now turn, is whether it is possible to reconcile facial scans as a kind of Fourth Amendment event within the defined limits of the previously discussed case law.

3. Facial Scanning, Consensual Encounters, and Implied Consent

A successful facial scan provides law enforcement with information about the individual that the computer has detected. As mentioned earlier, this information could be quite detailed or fairly minimal depending on the level of sophistication of the database.[126] Admittedly, the type of database being used will likely factor into the totality of the circumstances that define whether or not a seizure has occurred.[127] Nevertheless, we can proceed under the modest view that a local police station will have access to the following pieces of information: the name of an individual, the individual's social security number, the last-known address of the individual, the place at which the scan was obtained, the time at which the scan was obtained, and the criminal history of the individual scanned.[128]

Courts examining the specific moment at which a consensual encounter morphs into a seizure have repeatedly returned to the requirement established in *Mendenhall* and *Bostick* that an individual "feel free to decline the officers' requests or otherwise terminate the

124. *Id.* at 624.

125. *Id.* at 626.

126. *See supra* Part III.B.2.a.

127. For instance, a system that provided only a name match would be unlikely to rise to the level of a stop in the sense that I discuss below. But it is unlikely that such a system would be particularly valuable to law enforcement, because it provides no additional information that would be useful in preventing the commission of crimes.

128. As a practical matter, police are likely to have all of this information and more. Many states have in fact begun to put this information on-line for the general public. *See* Texas Department of Safety Crime Records Service, *Sex Offender Database*, at <http://records.txdps.state.tx.us/soSearch/soSearch.cfm> (last visited Apr. 1, 2003) (providing public information on the height, weight, sex, eye color, threat level, last-known address, and shoe size of various sex offenders).

encounter."[129] In practice, consensual encounters often begin by establishing the identity of the individual being questioned.[130] This initial moment of interaction between law enforcement officials and a potential suspect is the critical point at which the individual must assert her right to terminate the encounter because as soon as she accedes to the initial demand to identify herself, she may have already unwittingly provided enough evidence to rise to the level of reasonable suspicion.[131]

As for facial scanning, the same analysis applies. The moment at which the computer system recognizes an individual, ascertaining where she is at a particular time and tying that information to where she lives, her criminal record, and any other personal information available in the database, police may already have enough information to provide them with reasonable suspicion to satisfy the requirements of the *Terry* doctrine.

As my argument stands, however, there is still no reason to distinguish a facial scan from an ordinary consensual encounter between law enforcement and a suspect. For the purposes of situating my ongoing discussion, it is useful to establish a visual representation of what kind of governmental interventions we know about in order to determine where facial scanning might fit.

Level of Suspicion	**Governmental Intrusion**
Probable Cause	Custodial Arrest
Probable Cause	Quasi-Arrest
Reasonable Suspicion	*Terry* Stop
None	Consensual Encounter

From this chart we conclude that different types of interventions require different levels of suspicion in order to support the governmental intrusion. Facial scans are problematic in that they don't quite rise to the level of a *Terry* stop because there is no physical seizure, and yet, the facial scan itself engages in a kind of questioning without consent. As such, a scan is somewhere between a

129. *Bostick*, 501 U.S. at 436.

130. *See e.g., Mendenhall*, 446 U.S. at 547-48; *Bostick*, 501 U.S. at 441; *Florida v. Royer*, 460 U.S. 491, 494 (1983); *U.S. v. Hutchinson*, 268 F.3d 1117, 1118 (D.C. Cir. 2001); *U.S. v. Parra-Garcia*, 2001 U.S. App. LEXIS 106, at *5 (10th Cir. 2001).

131. For instance, Ms. Mendenhall's identification of herself, coupled with the discrepancy on her ticket, provided police sufficient reason to be suspicious that she might be a drug courier. *See Mendenhall*, 446 U.S. at 547-48.

consensual encounter and a *Terry* stop. Thus, a facial scan requires some level of suspicion greater than zero, yet less than reasonable suspicion, in order to be considered a valid Fourth Amendment event.

IV. An Alternative Approach

This article has repeatedly emphasized the difference between wide area scans and focused scans as tools of law enforcement.[132] This distinction is critical to finding an alternate solution that balances society's interest in preventing crime with the individual's interest in being free from governmental intrusions.[133]

This section first considers and rejects a state legislative solution to the problem of wide area scans before proposing a more comprehensive judicial solution.

132. *See supra* Part III.B.2.a.

133. *Terry*, 392 U.S. at 20-21 (citing *Camara v. Municipal Court*, 387 U.S. 523, 534-37 (1967)). ("[I]t is necessary 'first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen,' for there is 'no ready test for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails.'").

A. The Virginia Plan[134]

In response to the city of Virginia Beach's implementation of

134. Va H.B. 454, Leg. Sess. (Feb. 11, 2002). The bill provides, in part, that:

A. . . . no locality or law-enforcement agency shall employ facial recognition technology prior to complying with all of the provisions of this chapter.

B. The Attorney General or his designee, in any case where the Attorney General is authorized by law to prosecute or pursuant to a request in his official capacity of an attorney for the Commonwealth in any city or county, or an attorney for the Commonwealth, may apply to the circuit court, for the jurisdiction where the proposed facial recognition technology is to be used, for an order authorizing the placement of facial recognition technology by any law-enforcement agency in the jurisdiction, when the technology may reasonably be expected to provide (i) evidence of the commission of a felony or Class 1 misdemeanor, (ii) a match of persons with outstanding felony warrants, (iii) a match of persons or class of persons who are identifiable as affiliated with a terrorist organization, or (iv) a match of persons reported to a law-enforcement agency as missing. . . .

A. Each application for an order authorizing the use of facial recognition technology shall be made in writing upon oath or affirmation to the circuit court and shall state the applicant's authority to make the application. Each application shall be verified by the applicant to the best of his knowledge and belief and shall include the following information:

1. The identity of the applicant and the law-enforcement agency;

2. A full and complete statement of the facts and circumstances relied upon by the applicant in support of his request that an order be issued, including, but not limited to, (i) details either as to the particular offenses that have been, are being or are about to be committed, or the event or appearance that would attract individuals affiliated with a terrorist organization; (ii) a specific description of the nature and location of the facilities where or the place from which the facial recognition technology is to be used; (iii) a description of the type of match being sought; (iv) the identity of any persons or class of persons sought by the use of facial recognition technology . . . and (v) a description of the type of facial recognition technology to be used and a description of the contents of the database;

3. A statement of the period of time for which facial recognition technology is required to be maintained. However, in no case shall any request for an order granting the use of facial recognition technology be for longer than a period of ninety days; . . . .

B. If the court determines on the basis of the facts submitted that the provisions of this chapter have been met, and upon submission of a proper application, the court shall enter an order, as requested or as modified, authorizing the use of facial recognition technology within the territorial jurisdiction of the court. The application and any order granted or denied may be sealed by the court. . . .

9. The requirement that any facial image captured that is not relevant to (i) evidence of the commission of a felony or Class 1 misdemeanor, (ii) a match of persons with outstanding felony warrants, (iii) a match of persons or class of persons who are identifiable as affiliated with a terrorist organization, or (iv) a match of persons reported to a law-enforcement agency as missing shall be disposed of as soon as possible, but in no event be retained for more than ten days. . . .

A. The provisions of this chapter shall not apply to security measures undertaken at (i) public-use airports in the Commonwealth or (ii) harbors and seaports of the Commonwealth.

B. Any information acquired through facial recognition technology prior to July 1, 2002, shall be admissible in evidence in any suit, action or proceeding.

facial recognition technology at the Oceanfront, the State of Virginia House of Delegates passed a bill to severely circumscribe the use of the system.[135] Virginia's proposed scheme requires law enforcement officials to acquire authorization from the circuit court before installing scanning technology and only when the technology is reasonably likely to provide information pertaining to the commission of a felony, individuals with outstanding felony warrants, terrorists, or missing persons.[136]

In addition, the bill limits use of the installed system to 90 days, provides for court oversight, caps extensions to 60 days or less, and requires the deletion of images of all persons not falling into one of the four enumerated categories "as soon as possible, but in no event . . . for more than ten days."[137]

The text of the bill also provides for a series of exceptions to the requirements of the bill. First, the bill is not intended to curtail security measures taken to protect various ports of entry such as public airports and harbors.[138] In addition, the bill provides for a grace period during which time any evidence received from scans is admissible in court.[139]

While the House of Delegates' actions are certainly a step in the right direction, a number of problems remain with respect to privacy issues.[140]

First, although the bill enumerates four categories that would justify use of the scanning technology, the categories themselves are so broad that it would be virtually impossible for a court to deny them. In particular, because prediction of future activity is almost impossible absent explicit articulable facts, courts would likely have to rely on statistical analyses to justify the request. For instance, could a court reasonably deny a request to place scanners in an area where a large number of runaways had been apprehended previously using traditional methods? For that matter, should courts defer to

135. *Facial Scan: Beach's Use Restricted Under Bill Approved by House*, THE VIRGINIAN-PILOT & LEDGER STAR (Feb. 13, 2002) at B4, available at 2002 WL 5487250.

136. Va H.B. 454, Leg. Sess.

137. *Id.*

138. *Id.*

139. *Id.* (providing that "[a]ny information acquired through facial recognition technology prior to July 1, 2002, shall be admissible in evidence in any suit, action, or proceeding.").

140. Most notably, the chances that the bill will be ratified by the Virginia Senate is slim. *See supra* n. 98 ("The measure is expected to be passed by the full House next week but may have a tough time in the state Senate. Sen. Kenneth W. Stolle, R-Virginia Beach, vowed to vigorously oppose the legislation.").

police use of the technology in high crime areas? As a practical matter, local judges are unlikely to deny police department requests in all but the most exceptional cases.

Second, the fact that the bill controls the installation of the technology rather than the type of search is problematic. As discussed above, the real concern with wide area scans is that they cast an extremely wide net that brings a substantial number of individuals for whom there is no suspicion of criminal activity within the gaze of the state. Under the proposed bill, the arguably unconstitutional activity is limited in temporal duration but not in scope.

Third, to the extent that the bill requires a judicial decree each time that law enforcement wants to use its system, it unnecessarily hampers police from protecting society's interest in the effective investigation of criminal activity. Focusing on the type of search, rather than the type of technology employed, is a more appropriate solution.

Fourth, although the bill provides for the admissibility of evidence acquired from facial scans prior to the cut-off date, it does not explicitly provide for the exclusion of such evidence after the grace period. The only punishment for failing to comply with the bill is being held in contempt of court. Because the goal of exclusionary rules is to deter future police misconduct, any statute that failed to address this issue would likely be fatally flawed.[141]

B. The Judicial Option

Having discussed some of the pitfalls of one specific legislative solution, I consider what a judicially created solution might look like. In proposing this solution, I do not rule out the possibility that a legislative solution could provide some protection against the invasiveness of facial scanning; nevertheless, the judiciary's flexibility to deal with particular fact situations on a case-by-case basis may make it the superior forum for enforcing these rights.

My proposal is that the judiciary should recognize two types of facial scans: wide area scans and focused scans, sometimes known as one-to-one and one-to-many searches. As a general rule, the

141. *Dunaway v. New York*, 442 U.S. 200, 217-18 (1979) ("There are two policies behind the use of the exclusionary rule to effectuate the Fourth Amendment. When there is a close causal connection between the illegal seizure and the confession, not only is exclusion of the evidence more likely to deter similar police misconduct in the future, but also use of the evidence is more likely to compromise the integrity of the courts.").

judiciary should find that wide area scans are presumptively unreasonable searches of the person because they are supported by no level of suspicion. Nevertheless, law enforcement officials should be allowed to use facial scanning for focused searches so long as they believe that the use of such a scan is necessary to prevent the commission of a crime or aid in the investigation of a crime that has been committed. In practice, this could require police to have as little as a hunch, as to any particular person's potential involvement in criminal conduct, in order to justify the scan. The requirement would merely be intended to prevent wide area scans backed by no suspicion at all.

The goals of establishing such a system are twofold: first, it would reduce the number of individuals being processed and tracked by the system for whom there is no suspicion of involvement in criminal activity. Second, it would increase the probability that individuals who have committed or are about to commit a crime have a greater likelihood of being caught. In return, the increased likelihood of detection should deter future crime.

Management of such a scheme by the judiciary is essential, because the penalty for utilizing the scanning system in an authorized way will be the exclusionary rule. Because the scan will often be the first interaction between the police and the suspect, exclusion of all fruits of the initial search will act as a super-deterrent to illicit uses of the system.

V. Conclusion

The dystopic vision of a society in which the government tracks its individuals once seemed like the stuff of science fiction: the work of Orwell and Huxley, the abstract criticism of Foucault, the demented ramblings of conspiracy theorists. The truth is that the new millennium, pointedly ushered in by the attacks of September 11, has shifted the frame. This new world does more than ignore the cries of the lunatic fringe – it actively embraces the destruction of privacy under the guise of increased security. What is lost in this process is who we might need protection from: is it the next Joseph McCarthy? the next Hitler?

To the extent that one can resist the impulses of political fervor, the time is now. The incremental protections over which these battles are fought may not seem so incremental in retrospect. In this context, the oft quoted words of George Orwell, echoed in Justice Brennan's dissent in *Florida v. Riley*, ring eerily true:

> The black-mustachio'd face gazed down from every

> commanding corner. There was one on the house front immediately opposite. BIG BROTHER IS WATCHING YOU, the captain said . . . In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the Police Patrol, snooping into the people's windows.[142]

142. 488 U.S. 445, 466 (1989) (Brennan, J., dissenting) (*quoting* George Orwell, NINETEEN EIGHTY-FOUR 4 (1949).